UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

«ETUDE DE LA SÉCURITÉ DE SCHÉMAS DE CHIFFREMENT PAR BLOC ET DE SCHÉMAS MULTIVARIÉS» PAR JOANA TREGER

Présentée par : Mademoiselle Joana TREGER Discipline : Informatique Laboratoire : PRISM

La thèse se compose de deux parties. La première partie relate de l'étude de schémas de chiffrement par bloc, notamment les schémas de Feistel avec permutations internes et les schémas du type Misty. Le cadre de l'étude est générique, i.e. les permutations internes sont supposées aléatoires. Ceci permet d'obtenir des propriétés de la structure même des schémas, sans prendre en compte leur contexte d'utilisation. Cette partie focalise sur les attaques génériques sur ces deux schémas.

La deuxième partie concerne l'étude de cryptosystèmes multivariés. Une propriété de la différentielle de la clé publique du schéma HM est exhibée, fournissant un distingueur. Par ailleurs, une attaque par bases de Gröbner permet d'inverser le système efficacement. Nous exposons également une attaque sur le schéma HFE, permettant le recouvrement de la clé privée pour une famille d'instances particulières, classées à présent comme "clés faibles".

soutenance de thèse

Abstract :

The thesis is made up of two parts. The first one deals with the study of block cipher, Feistel networks with internal permutations and Misty-likeschemes. The context is generic, in the sense that the internal permutations are supposed random. This allows to obtain properties that only concern the structure of the scheme and do not depend on any particular application. This part focuses on generic attacks on these two schemes.

The second part is about multivariate cryptosystems. A differential property of the public key of HM is shown, allowing to get an efficient distinguisher. Moreover, we can invert the system by using Gröbner bases. We also describe a key-recovery attack on HFE, which works for a family of key instances, now called "weak keys".

Membres du jury :

Henri GILBERT, *Directeur de Recherche*, à Orange Labs Division Recherche et Développement - Issy-les-Moulineaux - Rapporteur

David NACCACHE, *Professeur des Universités,* à l'Ecole Normale Supérieure - Equipe de Cryptographie - Paris - Rapporteur

Jacques PATARIN, *Professeur des Universités, à l'Université Versailles Saint-Quentin-en-Yvelines/UFR des Sciences* - Laboratoire Parallélisme, Réseaux, Systèmes Modélisation (PRISM) - Versailles - Directeur de thèse

Jean-Sébastien CORON, *Maître de Conférences, Habilité à Diriger des Recherches*, à l'Université du Luxembourg - Faculté des Sciences, de la Technologie et de la Communication/Campus Kirchberg - Luxembourg - Examinateur,

Pierre-Alain FOUQUE, *Maître de Conférences, à l'Ecole Normale Supérieure* - Département d'Informatique - Paris - Examinateur

Eliane JAULMES, *Docteur,* à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) - Paris - Examinateur

Antoine JOUX, *Professeur Associé, à l'Université Versailles Saint-Quentin-en-Yvelines/UFR des Sciences - Laboratoire Parallélisme, Réseaux, Systèmes Modélisation (PRISM)* - Versailles - Examinateur

Dernière mise à jour de cette page : 18 février 2013